Risicomanagement in een geïntegreerde IT-omgeving

Risicomanagement in een geïntegreerde IT-omgeving

L.H.H. Bollen, R.H.J. Ronken, E.H.J. Vaassen[1]

1. Inleiding

Risico's die zijn verbonden aan het gebruik van informatie technologie (IT) vormen een dankbaar onderwerp voor menig artikel in de informatie management (IM) literatuur. Daarbij is er in het verleden met name aandacht besteed aan de risico's die samenhangen met de uitvoering van IT-projecten, met als belangrijkste insteek dat deze risico's een verklaring vormen voor de hoge falingspercentages van IT-projecten. Veel empirisch onderzoek binnen dit onderwerp heeft dan ook als doel tot een identificatie en classificatie te komen van de belangrijkste risico's rond systeemontwikkelingsprojecten (zie bijv. Barki, Rivard & Talbot, 1993; Keil, Cule, Lyytinen, & Schmidt, 1998; Sumner, 2000). In deze onderzoeken worden doorgaans risicofactoren genoemd zoals betrokkenheid van het topmanagement, projectcomplexiteit of de mate van technologische innovatie.

Veel minder aandacht is er in de IM literatuur gegeven aan de vraag welke risico's' er aan het gebruik van IT kleven op bedrijfsniveau in plaats van projectniveau. Om twee redenen heeft deze vraagstelling recent aan interesse gewonnen. Op de eerste plaats leidt de toenemende aandacht voor de corporate governance problematiek tot de vraag welke rol IT speelt bij het besturen en beheersen, en het daarover verantwoording afleggen aan belanghebbenden. Naar analogie van corporate governance willen regelgevende instanties door het uitvaardigen van richtlijnen voorkomen dat er op het terrein van IT excessen zullen optreden. Deze uitdaging is opgepakt door de Information Systems Audit and Control Association (ISACA), die in 1996 voor het eerst de Control Objectives for Information and Related Technology (COBIT) standaard heeft gepubliceerd. De aanbevelingen in dit rapport zijn inmiddels wereldwijd door een groot aantal organisaties overgenomen en COBIT is dé standaard geworden op het terrein van IT-governance (Vaassen, 2003a). De idee achter COBIT is dat het beheersen van IT-activiteiten een noodzakelijke voorwaarde is om de organisatiedoelstellingen te realiseren. Daartoe moet een balans worden gevonden tussen het managen van risico's en het realiseren van opbrengsten. Concreet betekent dit dat het management de belangrijkste IT gerelateerde activiteiten moet identificeren, de voortgang moet bewaken op de weg naar doelrealisatie, moet vaststellen in

[1] De auteurs zijn verbonden aan het departement Accounting en Information Management van de Faculteit der Economische Wetenschappen en Bedrijfskunde aan de Universiteit Maastricht. Correspondentie naar aanleiding van dit artikel kunt u richten aan Roel Ronken, e-mail: r.ronken@aim.unimaas.nl

hoeverre IT hieraan bijdraagt, en de beschikking moet hebben over instrumenten waarmee de organisatie kan worden afgezet tegen de 'industry best practices' en internationale standaarden.[2]

In het verlengde van de discussie rond corporate governance is er ook aandacht geschonken aan het concept Enterprise Risk Management, oftewel risicomanagement op bedrijfsniveau. Ook hier speelt vanzelfsprekend de vraag welke rol IT heeft in het totaalveld van bedrijfsrisico's. Aan deze vraag is in de IM literatuur eveneens veel minder aandacht besteed. De hierboven genoemde onderzoeksstroming naar de risico's van IT-projecten biedt hiervoor maar weinig aanknopingspunten, omdat projectrisico's wezenlijk anders zijn dan risico's op bedrijfsniveau. Slechts in het geval van bedrijfsbrede IT-projecten, waarbij de uitvoering van het project per definitie op bedrijfsniveau speelt, zijn die aanknopingspunten er wel. In recente jaren zijn het natuurlijk vooral de ERP-implementaties die het onderscheid tussen projectrisico's en bedrijfsrisico's gedeeltelijk doen vervagen. Veel ERP-implementaties hebben een dermate omvang dat een analyse van de risico's die met de uitvoering van deze projecten gepaard gaan gedeeltelijk overlapt met een analyse van risico's op bedrijfsniveau. Zo beargumenteren Campbell & Holland (2001) dat er bij ERP-implementaties, naast de risico's op projectniveau ook met risico's op bedrijfsniveau rekening moet worden gehouden, omdat deze mede het slagen van de ERP-implementatie bepalen. Daarnaast is het zo dat het geïntegreerde karakter van ERP-systemen ervoor zorgt dat dergelijke implementaties doorgaans meerdere onderdelen van de organisatie beïnvloeden. Ook hierdoor liggen projectrisico's vaak op het niveau van de organisatie als totaal. En daar waar het ERP-systeem wordt gebruikt als basis voor de inrichting van systemen tussen organisaties (interorganisationele systemen) zullen begrippen als projectrisico's en omgevingsrisico's dicht bij elkaar komen te liggen.

Het bewaken van de goede werking van een systeem, of het nu gaat om een informatiesysteem, een systeem van interne beheersing of willekeurig welk ander systeem, kan onder andere plaatsvinden door het periodiek laten doorlichten van het desbetreffende systeem. In het geval van een geautomatiseerd informatiesysteem, een belangrijke manifestatie van IT, kan een IT-auditor worden gevraagd deze doorlichting te doen. In de praktijk komt het echter vaker voor dat de controlerend accountant in het kader van de jaarrekeningcontrole het informatiesysteem beoordeelt als onderdeel van de beoordeling van de interne controle. Hier geldt dat hoe complexer het desbetreffende informatiesysteem, hoe groter de kans dat de accountant bepaalde

[2] Een recent onderzoek naar IT risk management binnen Engelse ondernemingen geeft aan dat er bij minder dan 20% van de respondenten sprake is van een formeel IT-risico framework en dat de belangrijkste stap die ondernemingen in dit kader willen nemen het integreren van het managen van IT-risico's en bedrijfsrisico's (80%) en het implementeren van IT-risicomanagement standaarden zoals COBIT (75%) betreft. (zie NCC, 2003)

IT gerelateerde risico's niet zal signaleren dan wel de zwaarte daarvan onjuist zal inschatten (zie o.a. Hunton, Wright & Wright, 2001).

In dit artikel gaan wij nader in op de identificatie en beoordeling van niet-projectgerelateerde IT-risico's op ondernemingsniveau. Daarbij gaan we allereerst in op de vraag hoe dergelijke risico's kunnen worden geclassificeerd en waardoor deze risico's worden beïnvloed. Daarbij zal in het bijzonder worden ingegaan op de vraag hoe de mate van integratie van de IT-omgeving van invloed is op de te onderkennen risico's. In het tweede deel van dit artikel wordt aan de hand van de resultaten van een experimentele studie ingegaan op de vraag in hoeverre accountants en IT-auditors, in het kader van de bewaking van de werking van systemen van interne beheersing (en dus ook risicomanagement) in staat zijn in een sterk geïntegreerde IT-omgeving accurate risico-inschattingen te maken. Uiteindelijk wordt in deze studie onderzocht wat het effect is van het systeemtype (geïntegreerd versus traditioneel) en deskundigheid (accountant versus IT-auditor) op de identificatie en beoordeling van verschillende typen IT-risico's.

2. IT gerelateerde risicofactoren

Accountants en IT-auditors maken gebruik van verschillende modellen om risico's in te schatten. Wellicht het meest gebruikte en bekendste risicomodel is het 'audit risk model', dat een hulpmiddel is voor accountants bij de controle van de jaarrekening. Dit model onderscheidt inherent risico, interne controle risico en detectierisico, waarna het cumulatieve effect van deze drie risicocategorieën wordt uitgedrukt als audit risk (zie bijv. AICPA, 1983). In het verleden is er kritiek geweest op dit model, die zich vooral richtte op de moeilijkheden die gepaard gaan met het kwantificeren van de risicocomponenten en de onafhankelijkheid van de risicocomponenten (zie bijv. Westra & Mooijekind, 1997). Gezien de huidige IT ontwikkelingen en het effect daarvan op de organisatie, rijst de vraag in hoeverre het audit risk model zich leent voor het inschatten van de risico's die samenhangen met de hoge inzet van IT binnen organisaties. Kinney gaf bijvoorbeeld in 1989 aan dat er door veranderingen in de omgeving, zoals bijvoorbeeld technologische ontwikkelingen, een meer compleet model van het audit risk moet komen (Kinney, 1989). Bell, Knechel & Willingham (1998) rapporteerden dat er duidelijke verschillen waren in de frequentie en oorzaken van fouten in een gecomputeriseerd accounting systeem in vergelijking met een handmatige omgeving (Bell et al., 1998). Hunton et al. (2001) geven tenslotte aan dat er in een geïntegreerde omgeving, zoals een ERP omgeving, sprake is van een aantal verhoogde risico's, zonder dat dit in het audit risk model tot uitdrukking komt. Gezien deze bevindingen is er behoefte aan een risicoclassificatie die betere mogelijkheden biedt de aan IT gerelateerde risico's in kaart te brengen.

Een alternatieve classificatie die beter rekening houdt met de risico's die voortvloeien uit het gebruik van IT is de classificatie van The Canadian Institute of Chartered Accountants (CICA, 1998). CICA definieert risico als iets wat de organisatie erbij hindert om haar bedrijfsdoelstellingen te realiseren. Risico's kunnen specifiek zijn voor een bedrijf, industrietak of locatie, maar kunnen ook ontstaan door het gebruik van technologieën zoals computers en communicatiemiddelen (CICA, 1998). Risico wordt binnen de CICA classificatie vervolgens opgesplitst in vier categorieën, zoals te zien is in figuur 1.

Een eerste overeenkomst tussen het audit risk model en de CICA classificatie is dat in beide gevallen inherent risico wordt beschreven. Volgens het audit risk model omvat het inherente risico zowel algemene als specifieke risico's (Westra & Mooijekind, 1997), daar waar de CICA classificatie een duidelijk onderscheid maakt tussen beide. Inherent risico wordt beschreven als het natuurlijke risico dat bestaat in een gegeven bedrijf of situatie en specifiek risico is het risico dat ontstaat tengevolge van de gekozen locatie of gebruikte processen in een bedrijf (CICA, 1998). Een tweede overeenkomst is dat er in beide modellen gesproken wordt over resterend risico. Volgens het CICA is dit het netto risico dat resteert na het implementeren van controles voor het verminderen van de eerder beschreven risico's (CICA, 1998), daar waar het audit risk model spreekt over detectierisico, gedefinieerd als de kans dat aan het interne controle systeem ontsnapte onvolkomenheden niet door de accountant ontdekt worden (Westra & Mooijekind, 1997).

[figuur 1 ongeveer hier invoegen]

Het grote verschil tussen beide modellen is echter de manier waarop IT en de daaruit voortvloeiende risico's opgenomen worden. Het audit risk model richt zich specifiek op het interne controle risico, ofwel het risico dat materiele fouten niet door het interne controle systeem worden gesignaleerd en gecorrigeerd (Westra & Mooijekind, 1997). CICA echter definieert technisch risico een stuk breder als de risico's die voortvloeien uit het gebruik van ondermeer IT om de bedrijfsdoelstellingen te realiseren (CICA, 1998). Dit laat zien dat de CICA classificatie een stap verder gaat in vergelijking met het originele audit risk model, omdat risico's voortvloeiend uit het gebruik van IT zich immers niet beperken tot de interne controle en de relatie met het financiële jaarverslag, maar op een bredere schaal bekeken en geïnventariseerd dienen te worden. De in het CICA model onderkende technische risico's worden verder uitgewerkt door Hunton et al. (2001). Mede op basis van een aantal focus groep bijeenkomsten met audit specialisten onderscheiden Hunton et al. (2001) vijf risicocategoriën, te weten risico's met betrekking tot applicatiebeveiliging, databasebeveiliging, netwerkbeveiliging, bedrijfsvoering en procesinterdependentie. Deze classificatie richt zich in het bijzonder op de risico's die ontstaan

tengevolge van de inzet van IT binnen het bedrijf. De classificatie van Hunton et al. (2001) is in het bijzonder geschikt om de effecten van IT in kaart te brengen. Hierna wordt specifiek aandacht gegeven aan de gevolgen van de inzet van ERP-systemen en de daarmee samenhangende integratie van databronnen en systemen.

3. Invloed van IT-integratie op risicofactoren

Met betrekking tot de mate van integratie van informatiesystemen wordt er in de literatuur gesproken van enterprise integratie, waarbij een bedrijf zich tot doel stelt een informatiesysteem infrastructuur op te zetten binnen de organisatie alsmede met externe partners (Noori & Mavaddat, 1998). Hieruit blijkt dat integratie op twee manieren bewerkstelligd kan worden, enerzijds middels internalisatie en anderzijds door middel van externalisatie. Internalisatie richt zich op het genereren van voordelen door het koppelen van interne systemen, bijvoorbeeld door het vervangen van losse maatwerkapplicaties door een ERP-systeem. Bij externalisatie is er sprake van de integratie van informatiesystemen tussen bedrijven, dit kan bijvoorbeeld middels het koppelen van een ERP-systeem met externe partijen (Lee, Siau & Hong, 2003). Figuur 2 toont een enterprise integratie matrix op basis van de twee dimensies. Binnen deze matrix worden vier verschillende vormen van enterprise integratie onderscheiden, gebaseerd op de mate van integratie. Stand alone vormt in dit geval de minst geavanceerde vorm, waarbij slechts sprake is van diverse, aparte informatiesystemen die binnen een bedrijf gebruikt worden. Volledig geïntegreerd vormt de meest geavanceerde vorm en hier is sprake van zowel internalisatie als externalisatie. Tussen deze twee uitersten zitten oplossingen die zich of alleen maar op richten op extern geïntegreerde systemen dan wel op intern geïntegreerde systemen.

[figuur 2 ongeveer hier invoegen]

Het is de vraag of de accountant zich bewust is van de veranderingen in risico's naarmate de mate van integratie stijgt. Als gekeken wordt naar de risicoclassificatie van Hunton et al. (2001) dan kan men zich voorstellen dat bijvoorbeeld het applicatierisico tamelijk basaal is en zal voorkomen in alle vier de kwadranten, maar dat dit risico in een meer geïntegreerde omgeving minder van belang zal zijn dan bijvoorbeeld het netwerkrisico of procesinterdependentierisico. Het ligt bijvoorbeeld voor de hand dat naarmate processen meer geïntegreerd raken, problemen in het ene proces hoogstwaarschijnlijk zullen leiden tot problemen in het daaropvolgende proces en dus een hoger procesinterdependentie risico zullen impliceren. In het hierna te bespreken onderzoek zal primair aandacht worden besteed aan de mate van internalisatie en de invloed daarvan op de risico-inschattingen door accountants en IT-auditors.

Een tweede factor die de invloed van IT op risicofactoren beïnvloedt is de manier waarop de accountant of de IT-auditor het systeem beoordeelt. Accountants vertrouwen veelal op ‘auditing around the computer’, een aanpak waarbij het systeem wordt gezien als een zwarte doos en de accountant een oordeel vormt middels een beoordeling van de gebruikerscontroles en een verificatie van de output. Echter naarmate het systeem gecompliceerder (bijvoorbeeld doordat er sprake is van meer integatie) wordt, zal er meer behoefte ontstaan aan ‘auditing through the computer’, waarbij het systeem meer inhoudelijk wordt beoordeeld. Verwacht kan woren dat technieken die deze laatste aanpak ondersteunen beter door IT-auditors worden beheerst en dat deze groep dus beter in staat zal zijn om geïntegreerde systemen te beoordelen. Dit heeft dus geen directe invloed op de risico’s die voortvloeien uit het gebruik van een geïntegreerd systeem, maar meer op de juiste inschatting van deze risico’s.

4. Risico-inschattingen door accountants in een geïntegreerde IT-omgeving

Deze paragraaf doet verslag van een onderzoek naar de reactie van accountants en IT-auditors op risicofactoren in IT-omgevingen met een hoge en een lage mate van integratie.

4.1 Onderzoeksmethode

Het onderzoek is gebaseerd op een experimentele studie waaraan 174 Nederlandse en Amerikaanse accountants hebben deelgenomen door het invullen van een vragenlijst. Het experiment is gebaseerd op een realistische case over een onderneming (Medical Solutions, Inc., een farmaceutisch bedrijf) waar respondenten als controlerend accountant de risico's moesten inschatten rondom het geautomatiseerde informatiesysteem. De case bevatte informatie over de cliënt, waaronder de omvang, de klantenpopulatie, de concurrentie, de controleomgeving, en de ervaringen van het accountantskantoor met de cliënt. Voor wat betreft het geautomatiseerde systeem waren er twee versies van de case: een traditioneel systeem en een ERP-systeem. Geprobeerd was het inherent risico en het frauderisico in beide versies gelijk te houden. Voorts werden de vragen in de cases in 'random-volgorde' gesteld om volgorde-effecten zo veel mogelijk te elimineren. Om een enigszins objectieve meting te verkrijgen van de prestaties van de proefpersonen werd een evidente controlezwakheid in beide versies van de case geïntroduceerd. Deze zwakheid betrof de toegang tot het netwerk, de databases, en de programmatuur. In een ERP-omgeving zou ongeautoriseerde toegang tot het systeem verdergaande consequenties moeten hebben dan in traditionele omgevingen. Voordat de case aan de eigenlijke proefpersonen werd voorgelegd is hij getest onder acht accountants en zeven IT-auditors om voldoende zekerheid te krijgen over de volledigheid en begrijpelijkheid van de case, de effectiviteit van de experimentele manipulatie, en de duidelijkheid van de genoemde risicofactoren en antwoordschalen. Op basis van deze test werden kleine aanpassingen aangebracht in de bewoordingen van enkele vragen en de achtergrondinformatie.

De doelstelling van het onderzoek was de effecten te onderzoeken van twee onafhankelijke variabelen: systeemtype (ERP versus traditioneel) en deskundigheid (accountant versus IT-auditor). De afhankelijke variabelen gaven de inschattingen weer van de unieke risico's verbonden aan het gebruik van ERP-systemen, waaronder storingen in de bedrijfsvoering, netwerkbeveiliging, databasebeveiliging, applicatiebeveiliging, procesinterdependentie, en controlerisico's. Voorts werd de proefpersonen gevraagd een indicatie te geven van hun vertrouwen in de kwaliteiten van de controlerend accountant om risico's in geautomatiseerde omgevingen in te schatten. Tenslotte werd hun de vraag voorgelegd of ze contact zouden opnemen met de IT-auditpraktijk van hun kantoor om aldaar de hulp in te roepen van IT-auditors ter ondersteuning van de controle. Bij elk van deze risico's werd tevens een vraag gesteld naar het vertrouwen dat de controlerend accountant had in zijn controleteam om effectief om te gaan

met deze risico's. In combinatie met het overzicht dat SAP hanteert om interrelaties tussen bedrijfsprocessen onderling en SAP-modules tot uitdrukking te brengen werd voorts een aantal vragen gesteld over de samenhang tussen de bedrijfsprocessen in de case. Tenslotte werd een aantal vragen gesteld die aansloten bij het formele risico-analysemodel zoals dat in de Statements on Auditing Standards is geformuleerd.

4.2 Resultaten

Allereerst is in het onderzoek nagegaan of de effecten van een geïntegreerde IT-omgeving terug te vinden zijn in risico-inschattingen die zijn gebaseerd op het traditionele audit risk model. De resultaten van deze analyse (zie tabel 1) geven aan dat met uitzondering van een enkele situatie, de risico inschattingen voor inherent risico, beheersingsrisico en frauderisico niet door de mate van integratie van de IT-omgeving worden beïnvloedt. Deze resultaten geven ofwel aan dat de mate van integratie van de IT-omgeving geen invloed heeft op de bedrijfsrisico's, ofwel de resultaten duiden er op dat het audit risk model minder geschikt is voor het meten van de effecten van een geïntegreerde IT-omgeving. Deze laatste verklaring is getest door accountants risico-inschattingen te laten maken op basis van het eerder genoemde model van Hunton et al. (2001).

[tabel 1 ongeveer hier invoegen]

De resultaten van dit onderdeel van het experiment kunnen als volgt worden samengevat (zie tabel 2). De invloed van de mate van integratie van de IT-omgeving (ERP versus traditioneel) wordt door respondenten aangegeven voor twee risicocategorieën, te weten risico's voor de bedrijfsvoering en het risico van procesinterdependentie. Respondenten blijken zich bewust van materiële, negatieve, financiële consequenties van computerstoringen in de ERP-omgeving in vergelijking met de traditionele IT-omgeving. Eenzelfde patroon was zichtbaar met betrekking tot de zorg die accountants hadden over de gevolgen van een computerstoring voor de voortgang in de bedrijfsvoering. Met betrekking tot de vragen over de interdependentie van de processen, het daarmee gepaard gaande risico dat problemen in het ene proces leiden tot problemen in een ander proces, en de daartoe getroffen preventieve beheersingsmaatregelen werd geconstateerd dat accountants onder de ERP-omgeving grotere risico's zagen dan in de traditionele IT-omgeving.

Voor de overige risicocategoriën (netwerkrisico, databaserisico, applicatierisico) worden geen significant andere risico-inschattingen door respondenten gemaakt. Zo zagen respondenten geen hogere risico's dat hackers van buiten de onderneming dan wel eigen medewerkers onbevoegd toegang tot het netwerk zouden krijgen in een ERP-omgeving. En in beide condities was men

ervan overtuigd dat de aanstelling van een netwerkbeveiligingsfunctionaris ertoe zou leiden dat de netwerkomgeving voldoende was beveiligd.

[tabel 2 ongeveer hier invoegen]

Met betrekking tot de invloed van de mate van deskundigheid (accountant versus IT-auditor) op de risico-inschattingen door accountants zijn de resultaten als volgt. IT-auditors maken systematisch grotere verschillen in risico-inschattingen in een ERP versus een traditionele omgeving in vergelijking met accountants. Dit resultaat geeft aan dat accountants in vergelijking met IT-auditors, de invloed van een geïntegreerde omgeving op de in te schatten risico's systematisch onderschatten. Wanneer respondenten echter wordt gevraagd naar de mate waarin zij zeker zijn van de door hen opgegeven risico-inschattingen dan blijkt niet dat accountants minder vertrouwen hebben in hun eigen vermogen de effecten van de mate van integratie in te schatten. Tevens blijkt dat accountants het doorgaans niet nodig achten het audit-team in een geïntegreerde IT-omgeving te versterken met extra IT kennis (bijvoorbeeld door het inschakelen van een IT-auditor). Beide resultaten geven aan dat accountants zichzelf heel goed in staat achten de risico's van een geïntegreerde versus traditionele IT-omgeving in te schatten, terwijl uit het de resultaten van de studie blijkt dat zij relatief weinig onderscheid maken tussen beide situaties als het gaat om risico inschattingen.

Aan het onderzoek hebben zowel Nederlandse als Amerikaanse accountants deelgenomen. Alhoewel over vrijwel de hele linie van het onderzoek Nederlandse accountants meer bezorgdheid tonen over de risico's voortvloeiend uit IT-integratie, zijn de hierboven beschreven resultaten geldig ongeacht de nationaliteit van accountants. De enige uitzondering vormt het effect van integratie op het beheersingsrisico (zie tabel 1). Dit risico wordt door Amerikaanse accountants hoger ingeschat in een geïntegreerde IT-omgeving versus een traditionele omgeving, waar Nederlandse accountants geen ander risiconiveau aangeven.[3]

5. Conclusies

In dit artikel is onderzocht hoe IT-risico's kunnen worden geclassificeerd en daardoor beter worden geïdentificeerd en beoordeeld. Omdat de beoordeling van risico's in het kader van de bewaking van de goede werking een onderdeel is van elk systeem van risicomanagement en omdat dit specifieke problemen met zich meebrengt in complexe geautomatiseerde omgevingen is in dit artikel nader ingegaan op de beoordeling van de IT-risico's door accountants en IT-auditors in ERP-omgevingen.

[3] Voor verdere details aangaande de verschillen tussen Nederlandse en Amerikaanse accountants verwijzen wij naar Vaassen (2003b)

De resultaten van deze studie kunnen erop duiden dat met name accountants in een door ERP-systemen gedomineerde IT-omgeving, bepaalde IT-gerelateerde risico's niet signaleren en derhalve onvoldoende controlewerkzaamheden zullen verrichten om te komen tot een deugdelijke grondslag. Deze problematiek wordt versterkt door het feit dat accountants aangeven zichzelf heel goed in staat te achten tot het maken van IT gerelateerde risico inschattingen. Aangezien accountants heden ten dage veelvuldig worden geconfronteerd met geïntegreerde informatiesystemen (ERP-systemen), moeten zij ten minste voldoende IT-deskundigheid ontwikkelen om een gefundeerd oordeel te kunnen vellen of er al dan niet een IT-auditor moet worden ingeschakeld. De resultaten van de studie geven aan dat accountants doorgaans weinig aanleiding zien om specifieke IT kennis aan het controleteam toe te voegen, ook niet als daar gezien de door henzelf gemaakte risico inschattingen wel aanleiding toe zou zijn. Het lijkt daarom evident dat deze problematiek de verdere aandacht van het accountantsberoep en de accountantskantoren vereist. Die aandacht zouden zij beter kunnen richten op het beter opleiden van accountants op het gebied van IT deskundigheid, het formuleren van betere procedures rondom het omgaan met een geïntegreerde IT-omgeving en het inschakelen van specifieke IT deskundigheid, maar ook in het ontwikkelen van betere risico modellen die het accuraat inschatten van IT gerelateerde risico's beter mogelijk maken.

Referenties

AICPA. (1983). *Statement on Auditing Standards No. 47 - "Audit Risk and Materiality in Conducting an Audit"*. New York: American Institute of Certified Public Accountants (AICPA).

Barki, H., Rivard, S., & Talbot, J. (1993). Toward an Assessment of Software Development Risk. *Journal of Management Information Systems, 10*(2), pp. 203-225.

Bell, T. B., & Knechel, W. R. (1998). An Empirical Investigation of the Relationship Between the Computerization of Accounting Systems and the Incidence and Size of Audit Differences. *Auditing: A Journal of Practice & Theory, 17*(1), pp. 13-38.

Campbell, M., & Holland, D. (2001). The two overlooked aspects of IT risk management. *Global Energy Business*(November/December), pp. 51-52.

CICA. (1998). *Information Technology Control Guidelines* (3de druk). Toronto: The Canadian Institute of Chartered Accountants.

Hunton, J. E., Wright, A., & Wright, S. (2001). *Business and Audit risks associated with ERP systems: Knowledge differences between information systems audit specialists and accountants.* Working Paper.

Keil, M., Cule, P. E., Lyytinen, K., & Schmidt, R. C. (1998). A framework for identifying software project risks. *Communications of the ACM, 41*(11), pp. 76-83.

Kinney Jr., W. R. (1989). Achieved Audit Risk and the Audit Outcome Space. *Auditing: A Journal of Practice & Theory, 8*(2), pp. 67-84.

Lee, J., Siau, K., & Hong, S. (2003). Enterprise Integration with ERP and EAI. *Communications of the ACM, 46*(2), pp. 54-60.

NCC. (2003). *Risk Management in IT*. Manchester: The National Computing Centre Ltd. (NCC).

Noori, H., & Mavaddat, F. (1998). *Enterprise integration: issues and methods.* International Journal of Production Research, *36*(8), pp. 2083-2097.

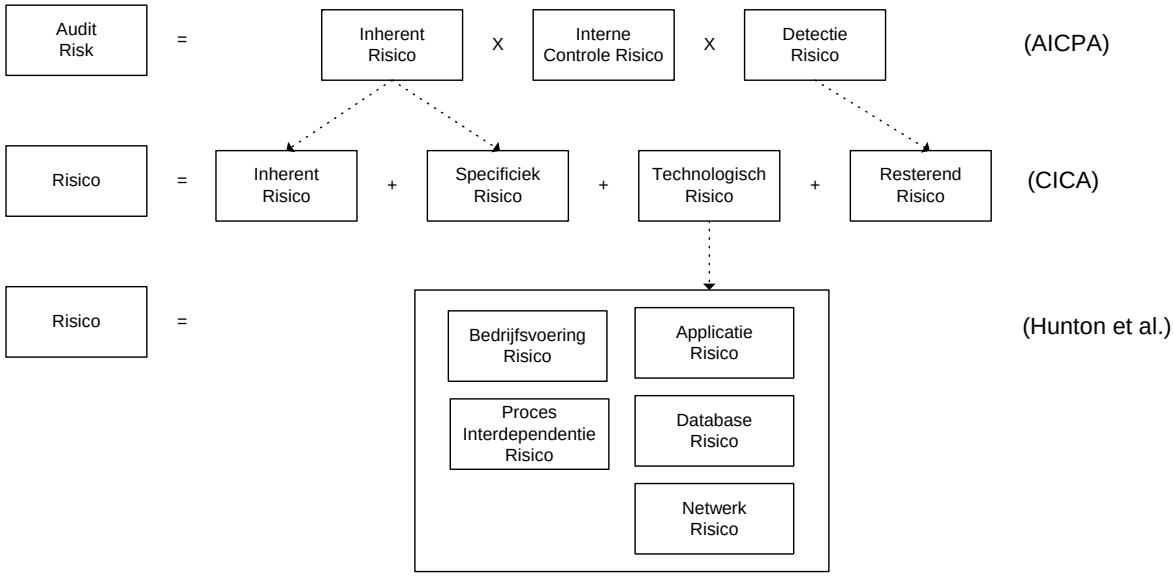
Sumner, M. (2000). *Risk factors in enterprise wide information management systems projects.* Paper gepresenteerd op de 2000 ACM SIGCPR conference on Computer personnel research, Chicago, Illinois.

Vaassen, E. H. J. (2003a). IT-governance. *Controllersjournaal*(November, 21), pp. 1-3.

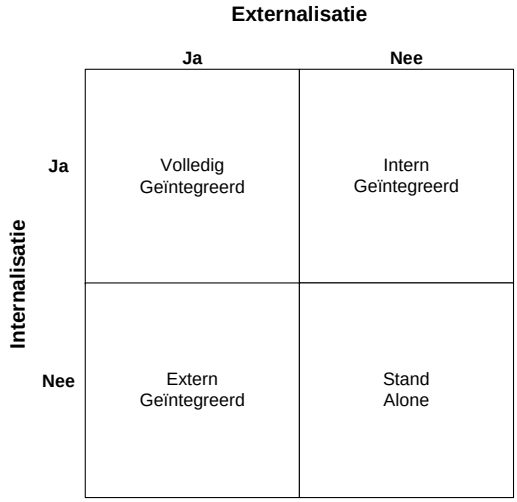
Vaassen, E.H.J., (2003b). *Risico-inschattingen door accountants in het kader van Enterprise Resource Planning-Systemen*. Maandblad voor Accountancy en Bedrijfseconomie *77*(11), pp. 509-520.

Westra, B. A. J., & Mooijekind, M. J. T. (1997). *Compendium van de Accountantscontrole, deel 1* (3de druk). Ede: Pentagan Publishing.

Figuur 1: Overzicht diverse risicomodellen en risicoclassificaties



Figuur 2: Enterprise Integratie Matrix



Tabel 1. Risico inschattingen door accountants in een ERP omgeving versus een traditionele IT-omgeving, op basis van het audit risk model[4].

Risicofactoren	**Accountants (N = 83)**	**IT-auditors (N = 91)**	**Totaal (N = 174)**
Inherent risico	Geen verschil	Geen verschil	Geen verschil
Beheersingsrisico	Hoger risico in ERP omgeving	Geen verschil	Geen verschil
Fraude risico	Geen verschil	Geen verschil	Geen verschil

[4] De in tabel 1 genoemde risico's zijn in het onderzoek elk met behulp van meerdere deelvariabelen gemeten. Indien in de tabel wordt gesproeken van een hogere risico inschatting dan geldt deze conclusie voor elk van de betreffende deelvariabelen. Van partieel hoger risico is sprake wanneer een significant hogere risico-inschatting is vastgesteld voor een deel van de deelvariabelen.

Tabel 2. Risico inschattingen door accountants in een ERP omgeving versus een traditionele IT-omgeving op basis van Hunton et al. (2001)[5]

Risicofactoren	**Accountants (N = 83)**	**IT-auditors (N = 91)**	**Totaal (N = 174)**
Bedrijfsrisico	Hoger risico in ERP omgeving	Hoger risico in ERP omgeving	Hoger risico in ERP omgeving
Netwerkrisico	Geen verschil	Partieel hoger risico in ERP omgeving	Geen verschil
Database risico	Geen verschil	Partieel hoger risico in ERP omgeving	Geen verschil
Applicatie risico	Geen verschil	Partieel hoger risico in ERP omgeving	Geen verschil
Procesinterdependentie risico	Partieel hoger risico in ERP omgeving	Hoger risico in ERP omgeving	Hoger risico in ERP omgeving

[5] De in tabel 2 genoemde risico's zijn in het onderzoek elk met behulp van meerdere deelvariabelen gemeten. Indien in de tabel wordt gesproeken van een hogere risico inschatting dan geldt deze conclusie voor elk van de betreffende deelvariabelen. Van partieel hoger risico is sprake wanneer een significant hogere risico-inschatting is vastgesteld voor een deel van de deelvariabelen.